Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously presented) A method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, wherein the wireless communication apparatus has memory means included within a separate unit comprising information to control the access of the wireless communication apparatus through a wireless communication network connected to the data communication apparatus, comprising:

connecting the wireless communication apparatus to the separate unit, accessing the wireless communication network connected to the data communication apparatus;

the wireless communication apparatus transmits a request to the data communication apparatus to establish a connection, the request comprising information of which at least one pre-defined algorithm the wireless communication apparatus supports;

upon reception of the request, the data communication apparatus chooses at least one algorithm associated with a public and a private key, and transmits a message back to the wireless communication apparatus, the message comprising the public key and information about which algorithm the data communication apparatus has chosen;

in response to the message comprising the public key, the wireless communication apparatus generates a master secret code and calculates a signature based on the chosen algorithm, the public key and the master secret code, and transmits a response to the data communication apparatus, the response comprising the calculated signature;

upon reception of the response comprising the signature, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received and the private key, and establishes a secure connection to the wireless communication apparatus, and saves the master secret code on the memory in order to re-establish the connection between the wireless communication apparatus and the separate unit

at a later occasion.

2. (Previously presented) A method according to claim 1, comprising saving the master secret code under a pre-defined time.

3. (Previously presented) A method according to claim 1, further comprising re-establishing the connection by transmitting a second request from the wireless communication apparatus to the data communication apparatus, the second request comprising the calculated signature based on the chosen algorithm, the public key and the stored master secret code, and upon reception of the second request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establishes a secure connection to the wireless communication apparatus.

4. (Previously presented) A method according to claim 1, comprising providing the memory means as a smart card.

5. (Previously presented) A wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, the wireless communication apparatus comprising:

communication means for establishing a connection to a wireless communication network connected to the data communication apparatus, memory means included within a separate unit provided with information to control the access of the data communication apparatus through the wireless communication network;

means for generating a master secret code in response to a message from the data communication apparatus;

control means arranged to use at least one pre-defined algorithm for generating a signature based on the master secret code and a public key received from the data communication apparatus, for use when the wireless communication apparatus establishes a secure connection to the data communication apparatus; and

the memory means comprises a secure database for storing the master secret code and the signature related to the data communication apparatus, in order to re-establish a secure connection to the data communication apparatus.

6. (Previously presented) A wireless communication apparatus according to claim 5, wherein the memory means is exchangeable.

7. (Previously presented) A wireless communication apparatus according to claim 5 wherein the master secret code is stored on the separate unit.

8. (Currently Amended) A wireless communication apparatus according to ~~any one of claims 5 to 7~~ claims 5 wherein the signature is stored on the separate unit.

9. (Previously presented) A wireless communication apparatus according to claim 5 wherein the master secret code is generated on the separate unit.

10. (Previously presented) A wireless communication apparatus according to claim 5 wherein the signature is generated on the separate unit.

11. (Previously presented) A wireless communication apparatus according to claim 5 wherein the separate unit comprises a smart card.

12. (Original) An apparatus according to claim 11 wherein the smart card is a subscriber identity module.

13.-14. Canceled.

15. (Previously presented) A memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, the memory card comprising being arranged to be connected to contact means, provided on the wireless communication apparatus, for providing information from the memory card to the wireless communication apparatus upon establishing a secure session to a data communication apparatus, the information is arranged to control the access of the data communication apparatus through a wireless communication network, and to save a calculated master secret code previously generated in response to a message previously

received from a data communication apparatus, in order to re-establish a secure connection to the data communication apparatus.

16. (Previously presented) A memory card according to claim 15, further comprising encryption means for encrypting the master secret, which is to be used as a signature for the wireless communication apparatus when the wireless communication apparatus is establishing a secure connection.

17. (Previously presented) A memory card according to claim 15, comprising a secure database provided with at least one of a master secret code and at least one signature related to at least one data communication apparatus, in order to reestablish a secure connection to data communication apparatus.

18. (Previously presented) A memory card according to claim 15, provided on a smart card.

19. (Previously presented) A system for establishing a secure connection when using a wireless application protocol, comprising:

a data communication apparatus based on the wireless application protocol;

a wireless communication network, connected to the data communication apparatus;

a wireless communication apparatus having memory means included within a separate unit comprising information to control the access of the wireless communication apparatus through the wireless communication network; wherein

the wireless communication apparatus is arranged to transmit a request to the data communication apparatus to establish a connection, the request comprising information of which at least one pre-defined algorithm the wireless communication apparatus supports;

upon reception of the request, the data communication apparatus is arranged to choose at least one algorithm, associated with a public key and a private key, and to transmit a message back to the wireless communication apparatus, the message comprising the public key and information about which algorithm the data communication apparatus will choose;

in response to the message, comprising the public key, the wireless communication apparatus is arranged to generate a master secret code, to calculate a signature based on the chosen algorithm, the public key and the master secret code, and to transmit a response to the data communication apparatus, the response comprising the calculated signature;

upon reception of the response comprising the signature, the data communication apparatus is arranged to calculate the master secret code based on the chosen algorithm, the signature received, and the private key, to establish a secure connection to the wireless communication apparatus; and

the memory means is arranged to save the master secret code, in order to re-establish the connection at a later occasion.

20. (Previously presented) A system according to claim 19, wherein the master secret is arranged to be saved under a pre-defined time.

21. (Previously presented) A system according to claim 19, the memory means is a smart card.

22. (Previously presented) A wireless communication apparatus for establishing a secure connection to a data communication apparatus through a wireless network based on a wireless application protocol, the wireless communication apparatus comprising:

means for establishing a connection with the data communication apparatus through the wireless network;

means for retrieving access information including which of a set of at least one pre-defined algorithm is supported, for transmission to the data communication apparatus;

means for processing information including a public key and selection of one of the at least one supported algorithm received from the data communication apparatus for storage;

means for retrieving a signature based on a generated master secret code and the public key received from the data communication apparatus, the generated master secret code

being generated in response to a message received from the data communication apparatus; and

means for utilizing the signature and the master secret code during communication with the data communication apparatus in order to re-establish a secure connection.

23. (Previously presented) A memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol and comprising contact means for cooperation with the wireless communication apparatus comprising:

a memory for storing a master secret code associated with the data communication apparatus and having been generated in response to a request from the wireless communication apparatus to provide such code for utilization of the master secret code during communication with the data communication apparatus in order to re-establish a secure connection.

24. (Currently amended) A wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, the wireless communication apparatus comprising:

communication means for establishing a connection to a wireless communication network connected to the data communication apparatus;

memory means provided with information to control the access of the data communication apparatus through the wireless communication network upon establishing a secure session to a data communication apparatus;

reading means for reading information received from the data communication apparatus and the information provided on the memory means;

means for generating a master secret code;

control means arranged to use at least one pre-defined algorithm for generating a signature based on the master secret code and a public key received from the data

communication apparatus, which is to be used when the wireless communication apparatus is going to establish a secure connection to the data communication apparatus; and

the reading means comprising a secure database provided with at least one of a master secret code and at least one signature related to at least one data communication apparatus, in order to re-establish a secure connection to a data communication apparatus.

25. (Previously presented) A method according to claim 2, further comprising re-establishing the connection by transmitting a second request from the wireless communication apparatus to the data communication apparatus, the second request comprising the calculated signature based on the chosen algorithm, the public key and the stored secret code, and upon reception of the request, the data communication apparatus calculates the master secret code based on the chosen algorithm, the signature received, and the private key, and, establishes a secure connection to the wireless communication apparatus.

26. (Previously presented) A method according to claim 2, comprising providing the memory means as a smart card.

27. (Previously presented) A method according to claim 3, comprising providing the memory means as a smart card.

28. (Previously presented) A wireless communication apparatus according to claim 6 wherein the master secret code is stored on the separate unit.

29. (Previously presented) A wireless communication apparatus according to claim 6 wherein the master secret code is generated on the separate unit.

30. (Previously presented) A wireless communication apparatus according to claim 7 wherein the master secret code is generated on the separate unit.

31. (Previously presented) A wireless communication apparatus according to claim 8 wherein the master secret code is generated on the separate unit.

32. (Previously presented) A wireless communication apparatus according to claim 6 wherein the signature is generated on the separate unit.

33. (Previously presented) A wireless communication apparatus according to claim 7 wherein the signature is generated on the separate unit.

34. (Previously presented) A wireless communication apparatus according to claim 8 wherein the signature is generated on a separate unit.

35. (Previously presented) A wireless communication apparatus according to claim 9 wherein the signature is generated on the separate unit.

36. (Previously presented) A wireless communication apparatus according to claim 6 wherein the separate unit comprises a smart card.

37. (Previously presented) A wireless communication apparatus according to claim 7 wherein the separate unit comprises a smart card.

38. (Previously presented) A wireless communication apparatus according to claim 8 wherein the separate unit comprises a smart card.

39. (Previously presented) A wireless communication apparatus according to claim 9 wherein the separate unit comprises a smart card.

40. (Previously presented) A wireless communication apparatus according to claim 10 wherein the separate unit comprises a smart card.

41. Canceled.

42. (Previously presented) A memory card according to claim 16, comprising a secure database provided with at least one of a master secret code and at least one signature related to at least one data communication apparatus, in order to reestablish a secure connection to data communication apparatus.

43. (Previously presented) A memory card according to claim 16, is provided on a smart card.

44. (Previously presented) A memory card according to claim 17, provided on a smart card.

45. (Previously presented) A system according to claim 20, the memory means is a smart card.

46. (Previously presented) A wireless communication device for receiving therein a separate unit with memory means, the device being operable to establish a secure connection with a data communication apparatus based on a wireless application protocol through a wireless communication network, the wireless communication device comprising: communication means for establishing the connection with the data communication apparatus, electrical contact means for communicating information between the communication means and the separate unit, the device being configured so that when the separate unit is received therein the resulting combination is operable to:

generate a master secret code in response to a message received from the data communication apparatus;

use a pre-defined algorithm to create a signature for use when the wireless communication device establishes a secure connection to the data communication apparatus, the signature being based on the master secret code and a public key received from the data communication apparatus; and

to store the master secret code and the signature related to at least one data communication apparatus in the memory means of the separate unit to enable re-establishment of the secure connection on a later occasion.

47. (Previously presented) A wireless communication device according to claim 46 operable when the separate unit is received therein to retrieve the at least one of at least one master secret code and at least one signature when re-establishing the secure connection on a later occasion.

48. (Previously presented) A wireless communication device according to claim 46 operable when the separate unit is received therein to cause both the generation and storage of the master secret code in the separate unit.

49. (Previously presented) A wireless communication device according to claim 47 operable when the separate unit is received therein to cause both the generation and storage of the master secret code in the separate unit.

50. (Previously presented) A wireless communication device according to claim 46 including a processor operable to generate the master secret code.

51. (Previously presented) A wireless communication device according to claim 47 including a processor operable to generate the master secret code.

52. (Previously presented) A wireless communication device according to claim 46 operable when the separate unit is received therein to cause the generation of the signature in the separate unit.

53. (Previously presented) A wireless communication device according to claim 47 operable when the separate unit is received therein to cause the generation of the signature in the separate unit.

54. (Previously presented) A wireless communication device according to claim 48 operable when the separate unit is received therein to cause the generation of the signature in the separate unit.

55. (Previously presented) A wireless communication device according to claim 49 operable when the separate unit is received therein to cause the generation of the signature in the separate unit.

56. (Previously presented) A wireless communication device according to claim 47 wherein the contact means are configured to receive the separate unit in the form of a smart card.

57. (Previously presented) A wireless communication device according to claim 48 wherein the contact means are configured to receive the separate unit in the form of a smart card.

58. (Previously presented) A wireless communication device according to claim 49 wherein the contact means are configured to receive the separate unit in the form of a smart card.

59. (Previously presented) A wireless communication device according to claim 50 wherein the contact means are configured to receive the separate unit in the form of a smart card.

60. (Previously presented) A wireless communication device according to claim 51 wherein the contact means are configured to receive the separate unit in the form of a smart card.

61. (Previously presented) A wireless communication device according to claim 52 wherein the contact means are configured to receive the separate unit in the form of a smart card.

62. (Previously presented) A wireless communication device according to claim 53 wherein the contact means are configured to receive the separate unit in the form of a smart card.

63. (Previously presented) A wireless communication device according to claim 54 wherein the contact means are configured to receive the separate unit in the form of a smart card.

64. (Previously presented) A wireless communication device according to claim 55 wherein the contact means are configured to receive the separate unit in the form of a smart card.

65. (Previously presented) A wireless communication device according to claim 46 wherein the contact means are configured to receive the separate unit in the form of a SIM card.

66. (Previously presented) A wireless communication device according to claim 47 wherein the contact means are configured to receive the separate unit in the form of a SIM card.

67. (Previously presented) A wireless communication device according to claim 48 wherein the contact means are configured to receive the separate unit in the form of a SIM card.

68. (Previously presented) A wireless communication device according to claim 49 wherein the contact means are configured to receive the separate unit in the form of a SIM card.